ARBRE ANALYSTE: UN OUTIL D'ARBRES DE DEFAILLANCES RESPECTANT LE STANDARD OPEN-PSA ET UTILISANT LE MOTEUR XFTA

ARBRE ANALYSTE: A FAULT TREE ASSESSMENT SOFTWARE FULLY COMPLIANT WITH OPEN-PSA AND USING XFTA FAULT TREE ENGINE

Emmanuel CLEMENT
Thierry THOMAS
Ligeron, Sonovision Group
23 rue Nicéphore Niepce
ZA de Loscoat, 29200 BREST
+33 (0)2 98 45 10 45
emmanuel.clement@sonovisiongroup.com
thierry.thomas@sonovisiongroup.com

Antoine B. RAUZY
Chaire Blériot-Fabre
Ecole Centrale de Paris
Grande voie des vignes
92295 Châtenay-Malabry
+33 1 41 13 10 25
Antoine.Rauzy@ecp.fr

Résumé

Arbre-Analyste est un nouvel outil libre de diffusion et d'utilisation dont le but est de standardiser et de pérenniser les modélisations par arbres de défaillances en s'appuyant sur deux piliers : le format Open-PSA et le moteur de calcul XFTA. Cet outil peut être employé dans les différents secteurs industriels pour lesquels une étude de sûreté de fonctionnement par arbres de défaillance est nécessaire. Arbre-Analyste permet d'éditer, d'afficher, de calculer, de traiter les résultats des calculs et d'exporter des arbres de défaillances vers différents outils de modélisation du marché.

Summary

Arbre-Analyste is a new freely redistributable software tool whose goal is to standardize and sustain fault tree models. It relies onto two pillars: the Open-PSA standard representation format on the one hand and the XFTA fault tree engine on the other hand. Arbre-Analyste can be used in all industrial sectors in which safety analyses by fault trees have to be performed. Arbre-Analyste allows edition, reviewing, calculation, export of the results of calculations and export of fault trees toward other tools of the market.

Introduction

Contexte

La complexité croissante des systèmes industriels amène un nombre toujours plus important d'acteurs à être impliqués dans les études de sûreté de fonctionnement. Plus que jamais, les modèles d'analyse du risque, typiquement les arbres de défaillance [1], doivent être partagés et maintenus dans le temps. Cela a deux conséquences importantes en ce qui concerne les outils d'édition et de traitement de ces modèles : d'une part, il devient impératif qu'ils soient interopérables, c'est-à-dire que leurs formats de sauvegarde soient identiques ou en tout cas compatibles. D'autre part, ils doivent être accessibles au plus grand nombre tout en ayant un très haut niveau de performance. La première de ces exigences ne peut être satisfaite que via la définition de formats standards. Le logiciel libre est un moyen de satisfaire la seconde.

Objectif

L'objectif de cette publication est de présenter un nouvel outil informatique libre de diffusion et d'utilisation dont le but est de standardiser et de pérenniser les modélisations par arbres de défaillance en s'appuyant sur deux piliers : le format Open-PSA [2] d'une part et le moteur de calcul XFTA [3] d'autre part. Cet outil peut être librement employé dans les différents secteurs industriels dans lesquels une étude de sûreté de fonctionnement par arbres de défaillance peut s'avérer nécessaire.

Problématique

Il existe, sur le marché, tout un ensemble de logiciels professionnels d'édition et de calcul d'arbres de défaillances. Malgré leur niveau de qualité élevé, ils ne permettent pas d'obtenir un niveau d'interopérabilité acceptable pour réaliser une étude de sûreté de fonctionnement entre différentes entités. Le standard Open-PSA a été conçu afin de résoudre ce problème. Cependant, peu de logiciels supportent encore ce format, et ceux qui le supportent ne le respectent pas strictement.

Approche

Nous présentons, d'un point de vue industriel, un nouvel outil de modélisation par arbres de défaillances libre d'utilisation et de diffusion. Ce nouvel outil s'appuie sur le standard Open-PSA, utilise le moteur de calculs XFTA et permet une interopérabilité avec les outils du marché. Par ailleurs, Arbre-Analyste est développé par des ingénieurs spécialistes du domaine de la sûreté de fonctionnement. De ce fait, l'ergonomie même du logiciel est optimisée pour la réalisation d'études de fiabilité et de sécurité. Les formats d'export permettent de faciliter l'étape de contrôle et le traitement des résultats des calculs. Les sorties graphiques sont compatibles avec des logiciels d'éditions graphiques et de traitements de texte afin de répondre au mieux aux besoins des bureaux d'études.

Notre présentation est articulée de la façon suivante :

1. Présentation du standard Open-PSA et de la façon dont il est supporté par Arbre-Analyste ;
2. Présentation du moteur de calculs XFTA ;
3. Présentation du logiciel Arbre-Analyste et de ses fonctionnalités ;
4. Présentation du cadre juridique du projet ;
5. Exemple d'application.

Le format Open-PSA

Présentation

Né en 2008, le standard Open-PSA [2] est un formalisme documenté permettant d'exprimer un modèle complet par arbres de défaillances. Il a pour principal but de permettre une parfaite interopérabilité entre les différents acteurs d'une étude.

Le choix du format de données s'est porté sur le XML (Extensible Markup Language). Le XML est un langage informatique de balisage générique. Cette syntaxe est dite « extensible » car elle permet de définir différents espaces de noms, c'est-à-dire des langages avec chacun leur vocabulaire et leur grammaire. L'objectif initial est de faciliter l'échange automatisé de contenus complexes (arbres, texte riche…) entre systèmes d'informations hétérogènes.

Exemple

Un exemple d'un arbre de défaillance traduit en Open-PSA est donné Figure 1.

Le moteur de calcul XFTA

XFTA est un moteur de calcul pour les arbres de défaillance [3]. C'est un logiciel libre, développé par l'un des auteurs dans le cadre de l'initiative Open-PSA. XFTA prend en entrée un modèle au format Open-PSA ainsi qu'un fichier décrivant les calculs à effectuer sur ce modèle, effectue ces calculs et affiche les résultats dans un ou plusieurs fichiers. Ce mode de fonctionnement permet de l'intégrer dans divers outils. Les fichiers de commandes obéissent à une grammaire XML, le format Open-PSA.

XFTA étant écrit en C++ ANSI, il est portable sous toute plateforme disposant d'un compilateur C++. Il est aujourd'hui porté sous Windows 32 et 64 bits ainsi que sous Linux 32 bits et 64 bits.

La version actuelle de XFTA implémente un algorithme extrêmement performant de calcul de coupes minimales (sans doute le plus performant disponible sur le marché). Cet algorithme s'appuie sur une énumération des coupes avec l'élimination au plus tôt de celles dont la probabilité est inférieure à un seuil donné.

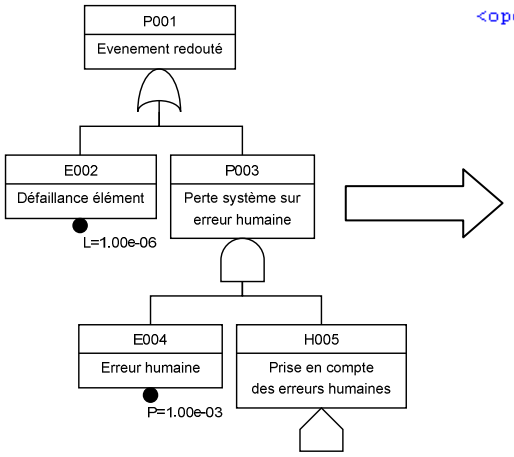
A partir des coupes minimales, XFTA implémente toutes les évaluations probabilistes classiques :

- Calcul de la probabilité de l'événement sommet ;
- Calcul de la probabilité des coupes minimales ;
- Calcul des facteurs d'importance des événements de base ;
- Approximation de la fiabilité du système ;
- Calcul de « Safety Integrity Level » ;
- Etudes de sensibilité via des simulations de Monte-Carlo.

Toutes ces évaluations peuvent être effectuées à différent temps de mission.

XFTA est aujourd'hui un outil complet. Il est prévu de le renforcer avec notamment :

- L'intégration d'un paquetage de diagrammes de décision binaires et les algorithmes d'évaluation qualitative et quantitative associés.
- Le développement d'outils connexes, notamment un moteur de calcul pour les chaînes de Markov multiphases à récompense ainsi des traducteurs permettant de transformer en arbres de défaillance (et chaînes de Markov) des arbres de défaillance dynamiques, des schémas blocs diagrammes, ou encore des arbres d'événements.




```
<open-psa>
    <label />
    <define-parameter name="P1" unit="float">
        <float value="1e-06" />
    </define-parameter>
    <define-parameter name="P2" unit="float">
        <float value="0.001" />
    </define-parameter>
    <define-gate name="P001">
        <label>Evenement redouté</label>
        <or>
            <basic-event name="E002" />
            <gate name="P003" />
        </or>
    </define-gate>
    <define-basic-event name="E002">
        <label>Défaillance élément</label>
        <exponential>
            <parameter name="P1" />
            <mission-time />
        </exponential>
    </define-basic-event>
    <define-gate name="P003">
        <label>Perte système sur erreur humaine</label>
        <and>
            <basic-event name="E004" />
            <house-event name="H005" />
        </and>
    </define-gate>
    <define-basic-event name="E004">
        <label>Erreur humaine</label>
        <parameter name="P2" />
    </define-basic-event>
    <define-house-event name="H005">
        <label>Prise en comptedes erreurs humaines</label
        <constant value="false" />
    </define-house-event>
</open-psa>
```

Explications des champs XML:

label : permet de décrire l'élément ;

define-parameter : permet de définir des paramètres nommés ;

define-gate : permet de définir des portes logiques ;

define-basic-event : permet de définir des éléments de base ;

define-house-event : permet de définir des éléments maisons

Figure 1. Le format Open-PSA

L'outil Arbre-Analyste

Présentation

Nous proposons donc un nouvel outil de modélisation par arbres de défaillances libre d'utilisation et libre de diffusion. Conçu par des ingénieurs spécialistes du domaine, il a comme objectif de permettre la capitalisation des modèles en proposant une parfaite interopérabilité. Pour cela, la libre diffusion du logiciel ainsi que l'utilisation du standard Open-PSA permettent à toutes les parties d'un projet l'accès aux modèles.

Interface

L'interface est conçue pour optimiser l'espace de travail et ainsi se concentrer sur l'édition des arbres de défaillances. L'emploi de menus détachables et de fenêtres flottantes permet d'organiser son espace de travail librement et de profiter de l'affichage multi-écrans.

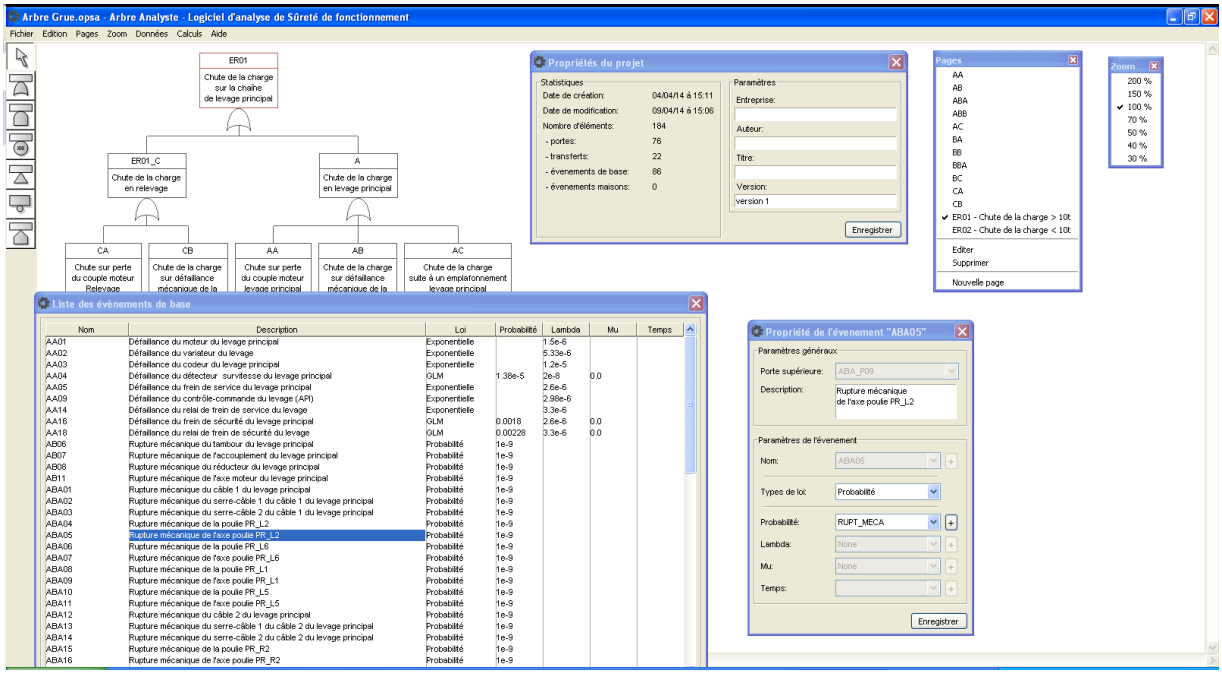


Figure 2. Copie d'écran l'interface graphique de Arbre-Analyste

L'interface permet d'éditer graphiquement le modèle sur des pages de type « infini ». Les arbres sont représentés à l'écran, tels qu'ils seront lors de leur exportation finale.

Calculs

Arbre-Analyste incorpore le moteur de calculs XFTA et permet ainsi de profiter, de façon transparente, de toute la puissance offerte par ce moteur de calculs. Ainsi, la phase préparatoire des calculs et la mise en forme des résultats sont réalisées de façon automatique par le logiciel.

Au moment de la rédaction de cet article, les lois de probabilité implémentées dans Arbre-Analyste sont :

- la probabilité constante ;
- la loi exponentielle ;
- la loi Gamma-Lambda-Mu.

De plus, les calculs réalisés sont :

- la probabilité de l'évènement de tête ;
- la fiabilité système ;
- le lambda système ;
- le nombre de pannes ;
- le MTTR système et le MTBF système ;
- la probabilité de chaque évènement de base ;
- les facteurs d'importance tels que les facteurs Birnbaum, Critical Importance Factor, Fussel-Vesely, Risk Increase Factor et Risk Decrease Factor;
- les coupes minimales, leur ordre, leur probabilité et leur contribution;
- la PFH, la PFD et la PFD moyenne ;
- les niveaux de SIL.

Arbre-Analyste comprend, en plus du moteur de calcul XFTA, un moteur de calculs par diagrammes de décision binaires qui permet ainsi, pour des arbres de taille modeste, d'obtenir la probabilité exacte. Cela permet, dans les rares cas où l'approximation par éléments rares donne un résultat trop majorant, d'obtenir une probabilité de tête juste.

Scénarios

Les systèmes étudiés, dans le cadre d'études de sûreté de fonctionnement, sont de plus en plus complexes et nécessitent de tenir compte des différents modes de fonctionnement du système ou bien de différents choix technologiques qui peuvent être employés. Cela nécessite de modifier l'architecture des arbres ou bien de modifier les paramètres des événements de base constituant l'arbre. Il existe, actuellement, deux solutions. Soit, on réalise autant d'arbres qu'il y a de situations différentes, soit en utilise des événements maisons. Les événements maisons permettent d'interagir sur l'architecture d'un arbre mais restent limités et complexifient la représentation graphique du modèle. Quant à réaliser autant d'arbres que de situations, cela peut rendre la modélisation complètement ingérable.

Arbre-Analyse propose une gestion de scénarios avancée permettant de modifier directement la structure et les événements des modèles afin de coller au mieux à la réalité des étapes de conception d'un système industriel.

La gestion des scénarios est réalisée par l'intermédiaire d'un langage simple et dédié aux arbres de défaillances. Il permet, grâce à un ensemble de sélecteurs et de fonctions, d'interagir dynamiquement avec les éléments de l'arbre.

Voici un exemple de l'utilisation d'un scénario :

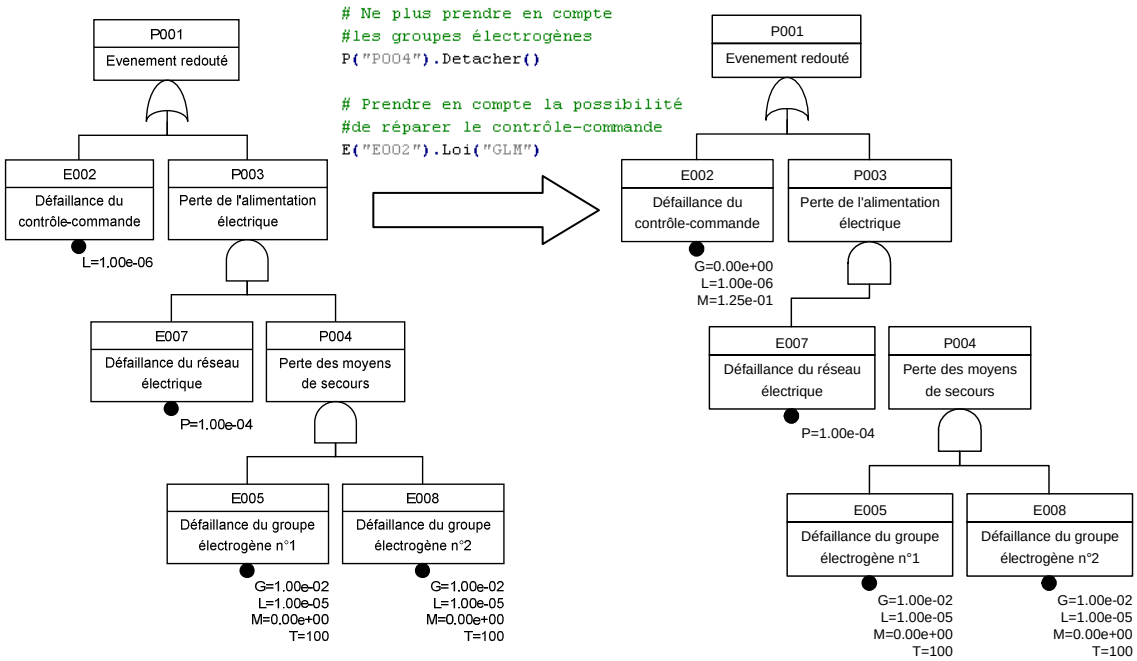


Figure 3. Exemple d'utilisation de scénarios

Le langage de scénario employé ici est basé sur le langage informatique « Python » [5]. Ce choix a été conditionné par la forte utilisation de ce langage dans le domaine de l'ingénierie. Il est ainsi possible de réaliser des scénarios avancés.

Voici, deux exemples d'utilisation avancés :

```
# Changement de la probabilité
# des évènements de bases "E010" à "E210"

compteur = 10

while compteur < 211:
    # Changement de la probabilité
    E("E%0.3i"%compteur).Probabilite("RUPTURE_2")
    # Incrémentation du compteur
    compteur = compteur + 1
```

```
# Modification de la loi de probabilité
# et du paramètre Lambda des évènements de base
# E002, E083, E120, E125 et E135

for element in ("E002", "E083", "E120", "E125", "E135"):
    E(element).Loi("Exponentielle").Lambda("RELAIS")
```

Imports et exports

Les systèmes industriels étant de plus en plus complexes, leur conception nécessite toujours de plus en plus d'acteurs. De ce fait, l'interopérabilité devient primordiale pour la réalisation d'une étude de sûreté de fonctionnement.

Arbre-Analyste est conçu de façon à être compatible avec les outils existants sur le marché. De plus, la compatibilité descendante est ancrée dans la politique même de développement du logiciel. Ainsi, les versions les plus anciennes des

modélisations réalisées avec Arbre-Analyse seront toujours pleinement compatibles avec les dernières versions dudit logiciel. La libre diffusion d'Arbre Analyste permet de s'affranchir d'une compatibilité ascendante tout en maintenant une parfaite interopérabilité.

Le cadre juridique et le futur d'Arbre Analyste

Afin d'assurer un avenir au logiciel Arbre-Analyste, une réflexion est en cours au sujet de la forme juridique à donner au projet. Plusieurs pistes sont à l'étude comme la création d'un club d'utilisateurs. L'idée étant de rendre le développement d'Arbre-Analyste plus communautaire et ainsi de répondre de manière plus précise et dynamique aux besoins des bureaux d'études.

Arbre-Analyste est encore au stade de développement actif, cependant, une version mature est déjà utilisable et en libre diffusion sur le site Internet du projet [4]. Elle permet de mener complètement une étude par arbre de défaillances. Des évolutions seront apportées par la suite afin d'améliorer le support des formats propriétaires, pour optimiser l'ergonomie même du logiciel ainsi que pour ajouter des fonctionnalités supplémentaires. Par exemple :

- compléter la liste des lois de probabilité ainsi que de logiques de portes ;
- permettre de saisir des lois de probabilité personnalisées ;
- ajouter les analyses de sensibilités et le calcul des incertitudes ;
- prendre en compte les causes communes de défaillances ;
- développer les scénarios afin de pouvoir mener des calculs itératifs pour, par exemple, mener des optimisations de maintenance par la fiabilité.

Il est prévu, par la suite, de traduire le logiciel dans différentes langues afin de faciliter son adoption.

Exemple d'application

Arbre-Analyste a été utilisé afin de réaliser une modélisation d'un réseau de distribution électrique dans le but d'en obtenir sa probabilité de défaillance ainsi que les différents facteurs d'importance des évènements de base.

Voici quelques informations à propos du modèle :

Nombre d'arbres	43
Nombre de portes logiques	429
Nombre d'évènements de base	428
Nombre de transfert	181
Nombre de coupes	1 339 681

Le temps de calcul, pour obtenir les différents résultats, a été de 1mn et 10 s sur un simple ordinateur de bureau.

Les coupes obtenues se repartissent de la façon suivante:

Ordre	Nombre
2	3
3	18
4	1 730
5	10 418
6	190 819
7	505 393
8	493 172
9	130 138
10	7 936

Toutes les analyses ont pu être menées de façon correcte et les résultats ont été comparés avec ceux produits par un logiciel du marché. Les résultats obtenus dans les deux cas sont exactement similaires.

Références

[1] IEC 61025, 2006, « Fault Tree Analysis »

[2] Epstein Steven, Rauzy Antoine, 12 mai 2008, « Open-PSA Model Exchange Format » disponible sur le site www.open-psa.org

[3] Rauzy Antoine, 15 octobre 2012, « XFTA | An Open-PSA Fault Tree Engine", disponible sur la page web de l'auteur www.lix.polytechnique.fr/~rauzy

[4] « Site Internet du projet Arbre-Analyste » : www.arbre-analyste.fr

[5] « Site Internet du langage Python » : www.python.org